NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND 20755-6000

PRESS RELEASE
24 June 1998
For further information contact:
NSA Public Affairs, (301) 688-6524

NSA RELEASES FORTEZZA ALGORITHMS

The National Security Agency today announced a decision to declassify both the Key Exchange Algorithm (KEA) and the SKIPJACK encryption algorithm. Both algorithms are used in the FORTEZZA PC card for key exchange and general purpose encryption, respectively, and the Escrowed Encryption Standard (FIPS 185) calls for the use of SKIPJACK. This decision will allow for the commercial development of lower cost, alternative smart card and software-based FORTEZZA products required to enhance the protection of sensitive but unclassified national security applications, while also assuring interoperability with the more highly protected mission critical applications.

The release is restricted to these two algorithms, SKIPJACK (an 80 bit encryption algorithm that is not extensible to higher key lengths) and KEA (a 1024 bit key exchange algorithm), and does not apply to any other classified NSA algorithms. The SKIPJACK and KEA algorithms and their source codes have been declassified pursuant to Executive Order 12958.

Declassification of the KEA and SKIPJACK algorithms is required to enable a software implementation in commercial FORTEZZA security-enabled applications. NSA is partnering with vendors to produce FORTEZZA toolkits to enable the availability of these applications.

The declassification of these algorithms is not intended to make them candidates for the Advanced Encryption Standard (AES) competition. NSA plans to support and use the eventual winner of that competition in appropriate DoD applications when it becomes available. Software FORTEZZA is a transition vehicle in migrating to AES based commercial security solutions for the Defense Information Infrastructure.

##